The privacy paradox applies to IoT devices too: a Saudi Arabian study

Noura Aleisa
Karen Renaud
Ivano Bongiovanni

The published article is available from doi:
https://doi.org/10.1016/j.cose.2020.101897

The Privacy Paradox Applies to IoT Devices Too: A Saudi Arabian Study

Noura Aleisa, Karen Renaud, Ivano Bongiovanni
[1] Saudi Electronic University
[2] Abertay University, Rhodes University
[3] University of Queensland

Abstract

The "privacy paradox" is the term used to describe the disconnect between self-reported privacy value attributions and actions actually taken to protect and preserve personal privacy. This phenomenon has been investigated in a number of domains and we extend the body of research with an investigation in the IoT domain. We presented participants with evidence of a specific IoT device's (smart plug) privacy violations and then measured changes in privacy concerns and trust, as well as uptake of a range of behavioural responses. Our Saudi Arabian participants, despite expressing high levels of privacy concerns, generally chose not to respond to this evidence with preventative action. Most preferred to retain the functionality the smart device offered, effectively choosing to tolerate likely privacy violations. Moreover, while the improved awareness increased privacy concerns and reduced trust in the device straight after the experiment, these had regressed to pre-awareness levels a month later. Our study confirms the existence of the privacy paradox in the Saudi Arabian IoT domain, and also reveals the limited influence awareness raising exerts on long-term privacy concern and trust levels.

1. Introduction

The recent, relentless expansion of the Internet of Things (IoT) has led to following forecasts: in 2025, IoT devices are expected to reach a staggering 75.44 billions, a nearly 146% increase from 2020 (30.73 billions) (Oshana and Kraeling, 2019). Whilst highlighting the magnitude of the IoT phenomenon, these numbers also raise concerns about the potential adverse consequences of the global roll-out of these networked devices. The research literature emphasises two kinds of concerns: *security* vulnerabilities (Cheruvu et al., 2019; Meneghello et al., 2019) and *privacy* violations (Gheisariy et al., 2019; Atlam and Wills, 2020). The research reported here focuses on the latter.

Owners of IoT devices can make setup decisions that will potentially jeopardise their privacy. This, in turn, can impact the privacy of others living in the

same dwelling. Many installation and setup decisions are influenced by the convenience intrinsic to IoT deployment such as, for example, in wearable devices (Kao et al., 2019), automotive industry (Kang et al., 2017), medical devices (Mavrogiorgou et al., 2019), and, on a larger scale, manufacturing (Ehie and Chilton, 2020), and smart cities (Ejaz and Anpalagan, 2019). All IoT devices claim to improve quality of life. Yet the unspoken reality is that they also collect a great deal of the owner's information (both public and personal, both consciously shared and unwittingly leaked).

Concerns have been expressed about IoT devices' potential to violate personal privacy. In 2019, global organisations Consumers International and the Internet Society surveyed consumers in Australia, Canada, France, Japan, the UK and the US about what matters most when buying connected devices. Findings highlighted that 75% of people distrusted the way data is being shared, 63% found data collection by connected devices "creepy" and 53% did not believe connected devices could effectively protect their privacy (Internet Society, 2019).

Intuitively, this type of evidence ought to result in an increase in behaviours aimed at protecting privacy. However, research has shown that this is often not the case (Hsu and Lin, 2016; Aleisa and Renaud, 2017b). This disjointedness between self-reported privacy concerns and actual privacy protecting behaviours has been termed the "privacy paradox" (Barnes, 2006; Norberg et al., 2007). When this manifests, those expressing concerns do not refrain from using privacy-violating devices, and rarely make an active effort to protect their own information (Gerber et al., 2018).

Nonetheless, research opinion related to the existence of the privacy paradox is not unanimous. Some studies question its nature (Trepte et al., 2014; Mohamed and Ahmad, 2012), leading Dienlin and Trepte to refer to it as a possible "relic of the past" (Dienlin and Trepte, 2015). Other scholars call for more experimental studies into this phenomenon (Barth et al., 2019). This call, the relative youth of the IoT field, and the potential of IoT devices to facilitate serious privacy violations (given that they are used within people's personal spaces), led us to carry out a study into the privacy paradox in the IoT domain.

Many privacy paradox studies have used surveys and interviews to gather evidence (Kim et al., 2019; Barth et al., 2019; Kitkowska et al., 2017; ten Berg et al., 2019; Williams, 2018). Yet Kraemer and Flechais (2018) argue that studies need to be carried out that merge interventions and observations to deliver greater insights into IoT-related privacy behaviours.

One of the aspects that is likely to influence these kinds of ethnologically valid studies is the environment, and particularly the privacy legislation that companies have to abide by. In Europe, the GDPR regulation (2018) provides strong privacy protection, and its influence will have pervaded society since it was imposed in 2018. To carry out this study, therefore, we decided to recruit participants in Saudi Arabia, where such legislation has not yet been enacted. This eliminated one possible confounding factor from our experiment and increased the originality of our investigation: Saudi Arabia has, in fact, not been the topic of such a study before.

We thus extend existing privacy paradox research with an experimental

study that: (1) raises awareness by showing people evidence of actual privacy violations by an IoT device, (2) measures privacy concern and trust levels after raising awareness and empirically observes actual behaviours in responding to the newly obtained knowledge of the privacy violation (Figure 1), (3) carries out the study in a context where the phenomenon has not been subject to an investigation before (Saudi Arabia), and (4) follows up with participants a month later to determine whether immediate post-experiment changes in privacy concern and trust levels have been sustained.

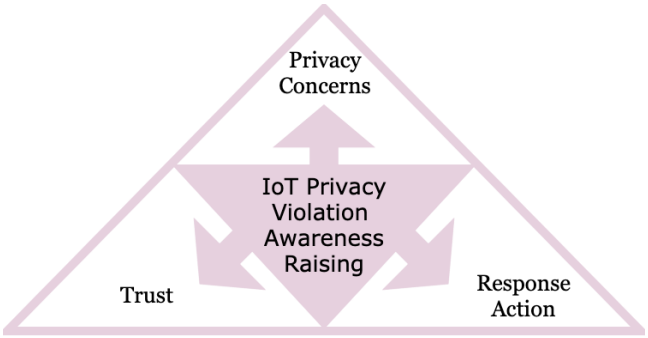

Figure 1: Studied IoT Privacy Paradox Constructs

The main purpose of this study was to unpack the relationships between privacy concerns, trust in one particular IoT device, privacy violation awareness and actions taken in response to such improved awareness in the Saudi Arabian context (both short and longer term).

Section 2 reviews the related literature. Section 3 then explains how we designed our study, with Section 4 reporting the results of our investigation and Section 5 discussing them. Section 6 concludes the paper.

2. Related Research

2.1. Privacy and IoT Devices Violating Privacy

In his seminal book "Privacy and Freedom", Alan Furman Westin defined privacy as "*the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others*" (Westin, 1967, p.7). This definition contains the basic components of privacy invasions: information about someone that is shared with others against their will.

The IoT network is considered particularly conducive to privacy invasions (Coulter and Pan, 2018). A 2013 study by Independent Security Evaluators (ISE) on the security of routers and Network-Attached Storage (NAS) devices was followed up by another similar study in 2019: the researchers found out that, in the 6-year timespan, no substantial improvements to device security were made (Mirani et al., 2019). Violation of privacy by IoT devices does not

only happen when vulnerabilities are exploited. In a study carried out on 81 consumer-based smart devices, it was discovered that 72 such devices shared data with third parties who were unrelated to the original manufacturers and all exposed information to eavesdroppers through plain-text flows (Ren et al., 2019). Consumer-based IoT devices were also the subject of investigation in a 2019 research project on Smart TVs and Internet-streaming devices (Mohajeri Moghaddam et al., 2019). By means of a smart crawler, researchers identified widespread user tracking and data collection in more than 2,000 "over-the-top" streaming channels. Data sent to tracking websites included MAC addresses, device serial numbers and video titles.

Poorly encrypted communications, inadequate user interfaces, or weak passwords often characterise the development of the IoT layers (sensors and data collectors; data transmission control; middleware; and application and services, (AlHogail, 2018)). Private device owners therefore run significant risks of privacy loss (Devarakonda et al., 2019; Chamarajnagar and Ashok, 2019). The next section looks at possible solutions.

2.2. Privacy-Protecting IoT Solutions

A number of viable solutions do exist and are available to consumers. For example, Dominikus (2011) proposed MedAssist, a privacy-preserving medical application that provides each consumer with full control over the right of access to their medical data. Henze et al. (2016) have introduced UPECSI (User-driven Privacy Enforcement for Cloud-based Services), a comprehensive approach that enables people to protect their data in transit to the cloud, and provides them with a user-friendly interface to configure privacy settings.

Companies who sell IoT devices utilise different strategies to raise consumers' awareness of their data collection and sharing practices. Privacy policies are among the most common of these. However, research has found that they are mostly ineffective, due to text complexity, lack of opt-out solutions, inadequate timing, utilised channels, varying audiences, and irrelevant data (Schaub et al., 2015).

Moreover, a systematic literature review (Aleisa and Renaud, 2017a) revealed that solution providers tend to assume two things. The *first* is that new owners will be aware of the IoT privacy-related issues, and the *second* that they will be willing to deploy one of the available privacy preserving solutions.

The overwhelming majority of the 83 solutions analysed by Aleisa and Renaud (2017b) mandated active end-user participation. The question that demands further examination is related to the extent to which people are aware of privacy violations and, if they become aware, whether they would use a tool that explicitly prevents such invasions.

2.3. Responses to Privacy Violations and the Role of Trust

IoT devices offer functionality benefits and enhance convenience and this influences their owners' privacy-protecting behaviours. Kim et al. (2019) investigated IoT devices in healthcare, smart transport and smart home services to

find that perceived benefit is positively associated with willingness to provide privacy information, whilst perceived privacy risk has no significant effect on such willingness (except for healthcare services). Zheng et al. (2018) conducted interviews with smart home owners and reported that the convenience offered by IoT devices influenced their privacy-related behaviours. Smart home owners also trusted IoT device manufacturers not to violate their privacy, but did not verify that this trust was warranted. Burgess et al. (2019) also carried out an investigation into consumer perceptions of the value of the data being leaked by IoT devices. They reported on a number of themes and highlighted the significant gap in consumers' understanding of what personal data is potentially being leaked, who owns it, and how IoT products are using their data. They argued for more consumer education and transparency in terms of how IoT owner data is being, and can be, used.

On the other hand, Barth et al. (2019) reported that even those with a heightened level of awareness of privacy violations continue to risk privacy intrusions. In fact, in line with the privacy paradox, privacy aspects did not inform their participants' use of apps, with functionality, app design and cost being the main predictors of app selection.

A construct closely associated with security and privacy, i.e. trust, reflects the confidence in, and expectations of, reliability, integrity, security, dependability, and ability of a piece of technology (Yan et al., 2014). In the field of IoT, user trust is a multi-faceted domain, with research that spans topics such as psychological aspects of risk, distrust, retaliation, altruism, association and brands (Køien, 2011).

Trust's influence on privacy concerns and behaviours has been well researched (Phelan et al., 2016; Barth et al., 2019). Its role has been modelled as a determinant or an outcome of concern; a mediator between concern and actual behaviours; and as a moderator of the influence of concern on actual behaviours (Smith et al., 2011). Trust assessment is a complex endeavour, as the literature generally acknowledges the multi-faceted nature of this construct, with assessable and non-assessable variables (Yan et al., 2014). The crucial role of trust in technology adoption dynamics has been stressed (AlHogail, 2018), specifically with regards to IoT products and services (Gao and Bai, 2014) and on third-party applications (Han et al., 2014).

The close relationship between privacy concerns, trust and information privacy behaviours (in the case of this study, privacy protection) is emphasised by Mayer et al. (1995), who defined trust as "*the willingness of a party to be vulnerable to the actions of another party based on the expectations that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party*" (p. 172). This definition is particularly relevant to this discussion, as it stresses the trade-off in which trust seems to play the role of fulcrum: on the one hand, an expected benefit (expectation of a particular action important to the trustor); on the other hand, a potential vulnerability (to the trustor's actions); in the centre: trust. In the dynamic environment of the digital age, technological affordances have enabled trust dynamics in a plethora of economic situations, to the point at which trust

has been named the currency of this new digital economy (Botsman, 2017). ten Berg et al. (2019) confirm the impact of trust, privacy concerns and perceived benefits on people's willingness to sacrifice their personal information in the IoT domain.

The concepts of privacy concerns, trust in, awareness of, and responses to, privacy violations summarised in this section have provided a framework for our research, which we will present next.

3. Investigation in the Saudi Arabian Context

3.1. Research questions, hypotheses and conceptual framework

The following three research questions (**RQ.X**), with associated hypotheses ($\mathbf{HX}_n$), are addressed and tested in this investigation:

RQ.A: ***Privacy Concerns*** — To what extent does a smart device owner's awareness of privacy violations impact their *privacy concerns* when using a device that does not require the upload of private data to enable its functionality?

If IoT device owners see evidence of IoT privacy violations, their privacy concerns related to smart devices will: not change ($\mathbf{HA}_0$) or increase ($\mathbf{HA}_1$).

RQ.B: ***Trust in IoT devices*** — To what extent does a smart device owner's awareness of privacy violations impact their *trust* in a smart device that does not require to upload private data to enable its functionality?

If IoT device owners see evidence of IoT privacy violations, their trust in the smart device will: not change ($\mathbf{HB}_0$) or decrease ($\mathbf{HB}_1$).

RQ.C: ***Chosen Response Action*** — To what extent does a smart device owner's awareness of privacy violations impact their *decision to act* to preserve their privacy, and *the nature of the action they take*. This, while using a smart device that does not require the upload of private data to enable its primary functionality?

If IoT device owners see evidence of IoT privacy violations, they will take no action to prevent them ($\mathbf{HC}_0$), take personal preventative actions (refusal, removal, misrepresentation) ($\mathbf{HC}_1$) or take public disapproval actions (direct complaint to 3rd parties, negative word-of-mouth, complaint to manufacturer) ($\mathbf{HC}_2$).

Figure 2 represents the conceptual framework of this investigation, where participants' awareness of IoT-related privacy violations is the independent variable (IV) and people's privacy concerns over IoT devices, their trust in IoT devices and responses to privacy violations are the three dependent variables (DVs).

3.2. Rationale

The experiment we report on here was carried out to determine the impact of improved privacy violation awareness, through an educational awareness presentation. According to Khan et al. (2011), this is the second most effective

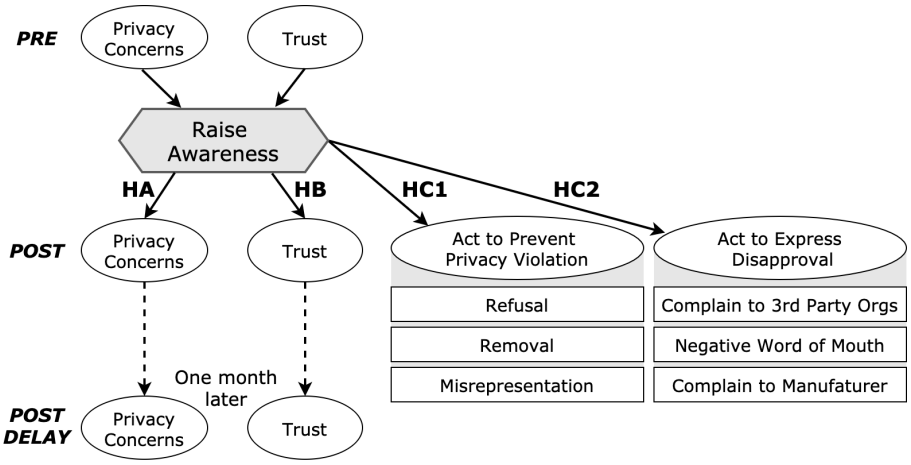

Figure 2: The conceptual framework of the present research.

way of increasing awareness. Increasing awareness about the consequences of personal information disclosure and providing individuals with privacy policies should increase transparency and reduce the privacy paradox. Any disparity between claims of privacy concerns and chosen actions will prove that the privacy paradox phenomenon manifests in the IoT domain (Williams et al., 2016). To this end, the research team purchased a smart plug. This device's only functionality is to switch itself on or off. Hence one can expect the device to generate very little network traffic, with the device only checking at regular intervals to determine whether it ought to be switched on or off, as appropriate.

We positioned the researcher's laptop so that it recorded all network traffic (see Figure 3). Our initial investigations showed that, contrary to expectations, the smart plug actually generated a great deal of traffic, much of which was transmitted to addresses that we could not identify using `https://whois.net`. It is reasonable to assume, *first*, that the device was not performing as it can reasonably be expected to, in terms of delivering its functionality. *Secondly*, we wanted to determine whether users would feel uncomfortable with the amount of data being transmitted by a device that ought only to receive and act upon on/off commands.

We asked participants in our experiment to use the smart plug for a 2 hour period. While they were doing so, we monitored all web traffic, and also attempted to resolve the IP addresses it communicated with. We then created a Web-based application to provide participants with an informative data traffic report at the end of their 2 hour stint. To complete the educational awareness presentation, we showed them the smart device's privacy policy. This allowed us to measure the impact of increased awareness of potential privacy violations.

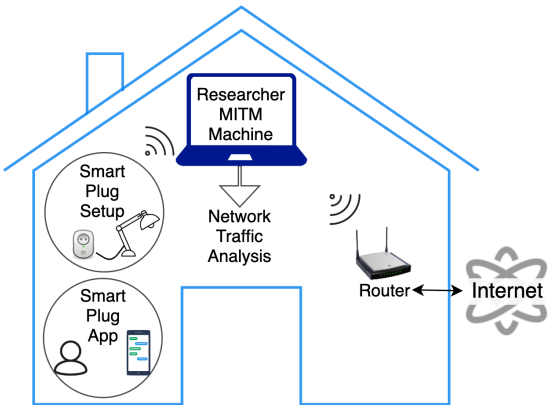

Figure 3: Smart plug monitoring setup.

3.3. Research Design

The goal of this study was to determine the impact of increased awareness of privacy violations associated to the usage of IoT devices on: (1) privacy concerns, (2) trust, and (3) actioned responses (Figure 1).

This study utilised a mixed-methods approach (Field, 2013), whereby data were collected through an interview (to introduce participants to the smart device used during the study and the related privacy policy, and recorded participants' responses), a questionnaire (to measure participants' trust in, and privacy concerns over, the IoT device, and the action they chose to take in response to their new awareness), and an observation (to observe and record whether the participants read the smart device privacy policy, and the amount of time they spent in doing so).

The target population was any smart device user over 18 years of age, of both genders, living in Saudi Arabia, a country chosen by virtue of three main factors.

First, Saudi Arabia experienced a recent increase in the number of owners of smartphones (Statista, 2019) (with smartphone penetration exceeding the international average (Thankappan, 2017)). This makes privacy violations an issue potentially affecting a large portion of population.

Second, a study conducted by Linksys in 2018 has revealed that there had been rapid adoption of IoT in Saudi Arabia and the UAE, with an increasing number of people consuming home smart devices (Telecom Review, 2018).

Thirdly, Saudi Arabia lacked privacy and data protection laws at the time this research was carried out. Only the Basic Law of Governance no: A/90 is applies to protection of the privacy of individuals (Wilkinson and Alsaab, 2019).

This allowed the research team to examine the relationships between the explored variables without the need to consider the mediating/moderating impact of privacy-related legislation.

3.3.1. Construct Measurement

This research utilised three well-established models to measure its DVs.

First, privacy concerns were measured using the Internet Users Information Privacy Concerns (IUIPC) (Malhotra et al., 2004) along three dimensions: (1) collection of, and (2) control over, personal information; and (3) awareness of organisational privacy practices.

Second, trust in IoT devices was measured using Cheung and Lee's instrument (2000) with minor modifications to match this study's design.

Third, responses to increased awareness of privacy violations were measured using the Information Privacy-Protective Responses taxonomy (IPPR, with adaptations to the field of IoT) (Son and Kim, 2008). In its original formulation, this taxonomy is also a nomological model that classifies potential behavioural responses into three categories and six types:

- *No action.*
- *Personal action — prevention*: with one of: (1) *refusal* (block all traffic to unusual IP addresses), (2) *removal* (remove personal information), or (3) *misrepresentation* (falsify the personal information they exchange).
- *Public action — disapproval:* with one of: (1) *complain to 3rd parties* (send an email to the third-party organisation involved in the privacy violation to voice their concerns), (2) *negative word-of-mouth* (voice their concerns to friends/ relatives), or (3) *direct complaint to manufacturer* (send an email to the smart devices' manufacturers to voice their concerns).

3.3.2. Experiment Steps

The experiment conducted in this study had three phases (Figure 6):

Phase 1 (Preamble): Participants:

1. read and signed the consent form.
2. were introduced to the smart device used in the experiment: a smart plug to connect a table lamp to the WiFi network. They could switch the lamp on and off using a smartphone app.
3. were provided with the smart device policy (Figure 4). The researcher recorded whether participants read the policy, and, if so, how long they spent doing so.
4. were given an open-ended "pre-awareness" questionnaire to record their privacy concerns, using the IUIPC (Malhotra et al., 2004); Participants were then given an open-ended questionnaire to record their level of trust in the IoT device, using questions adapted from Cheung and Lee (2000).

"This Privacy Policy covers how we treat 'Personal Information', that we collect during your use of our Services. This Policy does not and cannot cover the practices of companies, third parties, and individuals that we do not own or control, or people that we do not manage. During your use of the Services, we will gather Personal Information from our users and will use this information in connection with the Services. The information is used to deliver the basic functionality of the Services, to offer personalization of the Services, to contact you or have other users contact you, to analyze how you use the Services, to allow you to create, modify, and view your account information, and to allow you to customize, rate, and review the Services. In certain cases as defined below, we may also share some Personal Information with third parties. We receive and store the information you knowingly provide to us. During account registration or account update, this can include your name, email address, shipping and billing address, mobile, home, work phone numbers, credit card information or credit card processing information, names you give to your locations, geo-fenced location, names of users for your account, device names, device location names, device group names, scene names, device images, location images, user images, device configuration details, third party account credentials, schedules for devices or groups, and names of schedules."

Figure 4: The Privacy Policy

Phase 2 (Experiment): The researcher installed her own PC as a man-in-the-middle device to monitor all network traffic. A software application was used to monitor the network traffic sent out or received by the smart device mechanism (smart plug and smartphone) for two hours.

Participants chose to engage in either path (A) and (B), and both saw a traffic analysis report based on data collected by the smart device and shared with third-party companies (via unusual or unknown IP addresses). This report depicted network traffic both when the smart device was, and was not, in active use (one hour each).

The software on the researcher's computer analysed the network traffice and produced a detailed report on IP addresses (source and destination), number of packets, total size, and host name of each packet (Figure 5).

Participants were asked whether they wanted to install the IoT device application on their own smartphone to operate the lamp. Either, they:

(A) agreed to install the application. In this case, the participant:

  (i) installed the app on their own Smartphone.

  (ii) was prompted at random intervals to switch the lamp on and off, to ensure that network traffic was generated during the first hour. During the second hour, the participant did not use the smart device to switch the light on or off. They continued to use their own device for normal activities. Network traffic was monitored and recorded throughout the two hours.

  (iii) was shown the analysis of their own network traffic.

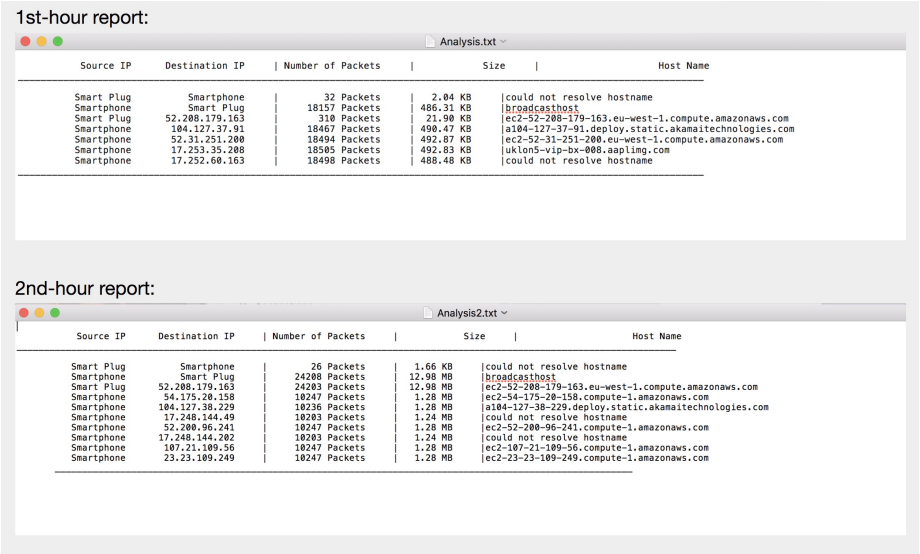

Figure 5: The Researcher's Data showing Volume and Destination of Traffic.

(B) did not agree, and the researcher's data was used as evidence of IoT device activity. In this case:

(i) the researcher used the smart device's functionality at random intervals from her own Smartphone to make sure that network traffic was generated during the first hour. During the second hour, the researcher did not actively use the smart device. Network traffic was monitored and recorded throughout the two hours.

(ii) the participant was shown the analysis of the researcher's network traffic.

The experiment concluded with a final four steps. The participant:

(i) was introduced to the smart device privacy policy. This, together with their awareness of evidence of actual network traffic reflecting privacy invasion, ensured that they were well informed of actual as well as stated privacy violations perpetrated by by the smart device.

(ii) completed the privacy concern and trust questionnaires.

(iii) indicated their chosen response to the increased awareness.

(iv) gave feedback on the experiment and asked any questions they wanted to ask.

Phase 3 (Follow Up): A month later, those participants who had consented were contacted and once again completed the privacy concern and trust ques-

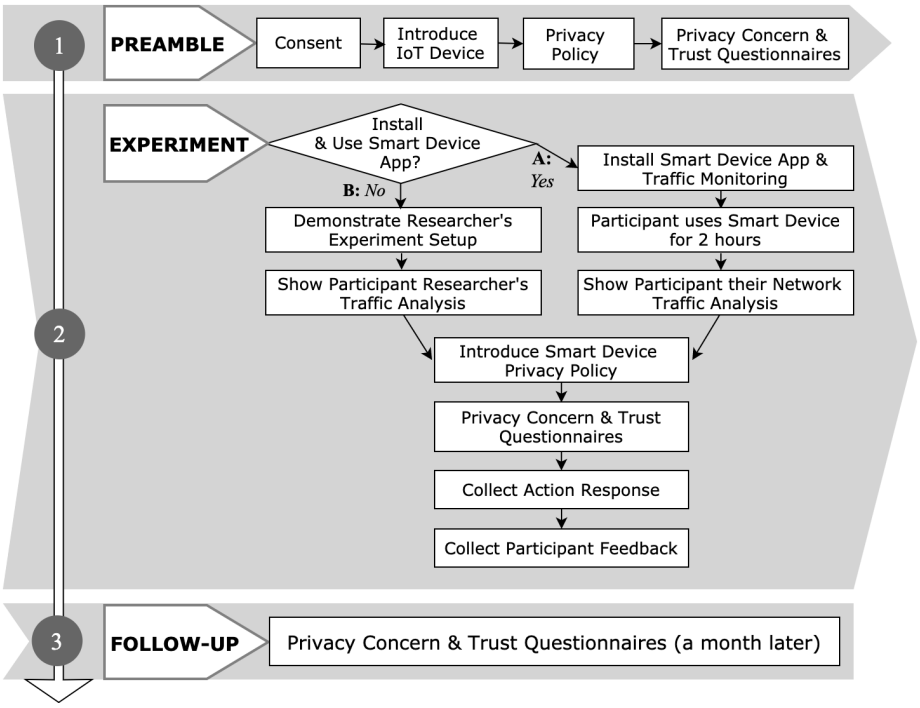

Figure 6: The Experiment Flow

tionnaires.

3.4. Validity, Reliability and Data Analysis

Content validity of the questionnaires (Field, 2013) was ascertained by administering all the questionnaires to a questionnaire construction expert who checked for common errors, such as double-barrelled, confusing, ambiguous, and leading questions (Field, 2013). Two experts then examined the questionnaires and provided comments on the clarity of the questions. Comments included, for example: "*I looked through the survey, and some of the questions were priming people to answer*" and "*I can see a lot of thought went into this. It is looking good*". Finally, three people with no technological expertise completed the questionnaires while passing on their comments.

The experiment's content validity was tested via internal and external validity measures (Field, 2013). The internal validity ensured that the independent variable (awareness) influence the dependent variables (trust level, privacy concerns, and response). It was performed by asking two people with no technological background (test group) to conduct the experiment and provide the researcher with feedback to help improve the content and the process flow of the experiment. Their results were also used to check whether the designed instrument actually measured what it was set out to measure. The researcher found

from the results of the test group that the unfamiliarity with the smart device would influence the DVs. To reduce this, the researcher would introduce the smart device (smart plug) and ask the participant to try it before commencing with the experiment.

External validity is concerned with whether the outputs of the study can be generalized to the target population, and the randomization needs to be granted by ensuring that gender, age, technological background, education are variable in the test group. In this study, three random people (test group) were asked to engage with the experiment, and their results were tested to verify generalizability.

Well-established measurements instruments drawn from the research literature were utilised in the present study (IUIPC) (Malhotra et al., 2004); Cheung and Lee's instrument (Cheung and Lee, 2000); and IPPR (Son and Kim, 2008), which corroborates measurement validity. To verify reliability of the utilised instrument, two randomly selected individuals were asked to conduct the experiment and answer all the questionnaires twice. The outputs were checked for similarity (test-retest reliability) and the relationship between the results of the repeated tests were positively correlated (Field, 2013).

Collected data were stored in a MySQL database and then analysed using IBM SPSS. Data analysis was carried out in two ways. The IV was manipulated using the same entities and repeated measures design (Salkind, 2010). The same group of participants were tested in their statistical perception. First, without giving any information on their privacy whilst using a smart device; second, giving them precise information on their privacy whilst using a smart device; and finally, assessing their privacy concerns a month later by completing a trust and privacy concerns open-ended questionnaire through email (Field, 2013). Second, collected data on participants' responses to privacy violations were analysed by manipulating the IV using different entities. Two groups of participants had their awareness of privacy violations during usage of the smart device increased by the researchers. Their responses to such violations were measured and statistical analysis performed, testing the correlation between the measured variables using a non-parametric Spearman's correlation (Field, 2013).

3.5. Research Sample

A convenience sampling technique was employed by using volunteers as research participants (Bell et al., 2018). A total of 46 individuals (36 male, 10 female; with educational backgrounds ranging from high school to doctoral studies) participated in the experiment.

Of the 46 participants, 20 agreed to download the smart device app on their own smartphone (therefore utilising their own data for the experiment) and 26 opted to utilise the researcher's home experiment. Thirty-four agreed to be contacted one month after the experiment to once again measure privacy concerns and trust in the IoT device after a month's delay.

The size of this sample was considered appropriate based on the fact that the experiment took two hours, a duration that would usually discourage participation and reduce the number of individuals in an experimental sample.

3.6. Privacy Concerns and Trust Measurements

Having ensured that the questionnaires were validated, each participant's privacy concerns using the IoT smart device were measured three times: (1) before the commencement of the experiment, (2) after making participants aware of the privacy violations committed by the smart device (n=46), and (3) a month after the end of the experiment (n=34), using the IUIPC 10-item scale (Malhotra et al., 2004). A seven-point Likert scale was used, ranging from 1 (minimum concern) to 7 (maximum concern).

Similar to privacy concerns, each participant's level of trust in the IoT smart device was measured before and after making participants aware of the privacy violations perpetrated via the smart device, and a month after the end of the experiment, using Cheung and Lee's 13-item scale instrument (Cheung and Lee, 2000). A seven-point Likert scale ranged from 1 (minimum trust) to 7 (maximum trust).

4. Results

None of the participants read the privacy policy provided with the smart device during the experiment preamble. The preamble was implemented as a sequence of web pages, which participants could complete or click through, as they preferred.

4.1. ***RQ.A: Privacy Concerns***

Our findings highlight the fact that participants had high levels of concern about their data across the three categories of privacy concerns, namely (1) control, (2) awareness of privacy practices, and (3) data collection, even before the researcher disclosed privacy violations perpetrated by the smart device (avg=5.86957).

Concerns increased slightly when the participants were made aware of the smart device privacy violation (avg=6.15651) and decreased slightly, even below pre-awareness levels, a month after the experiment (avg=5.77942). Figure 7 illustrates participants' privacy concerns. The vertical axis reflects the score on the seven-point Likert scale, while the horizontal axis corresponds to the measurement instrument questions.

An analysis of the differences around privacy concerns between participants (n=20) who agreed to utilise their own smartphone (i.e. their own data) and those who opted to utilise the researcher's data (n=26) demonstrated that privacy concerns before awareness were basically the same. However, participants who generated their own data visualisation demonstrated significantly higher levels of privacy concern after awareness; such concerns slightly decreased a month after the experiment, yet stayed higher than the other group's (Figure

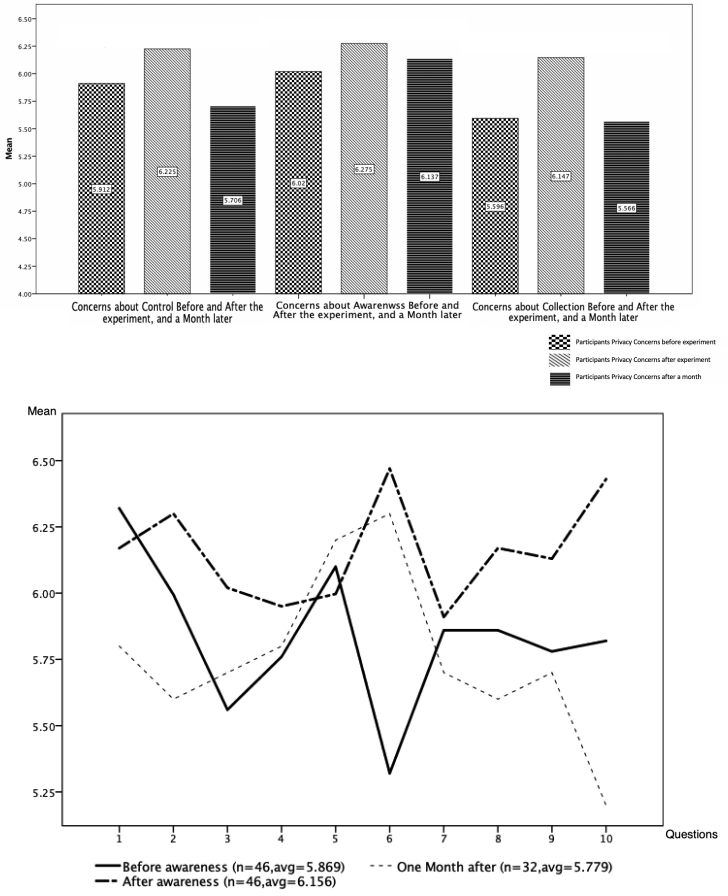

Figure 7: The privacy concerns before, and after the experiment.

8). The reason for the minor increase in the participants' privacy concerns could be due to these participants already being aware of IoT privacy issues. The precise information provided during the experiment made them even more aware of the potential privacy violations related to the specific IoT device (Smart Plug).

4.2. ***RQ.B: Trust in IoT devices***

The responses demonstrated a very significant decrease in trust (avg=2.66052) as compared to before they became aware of the privacy violations perpetrated by the smart device (avg=5.18729). Trust levels increased when measured again a month after the experiment, but not to initial levels (avg=4.78732). Figure 9 illustrates participants' trust in the IoT smart device: the vertical axis reflects the score on the seven-point Likert scale, while the horizontal axis each of the thirteen questions of the measurement instrument.

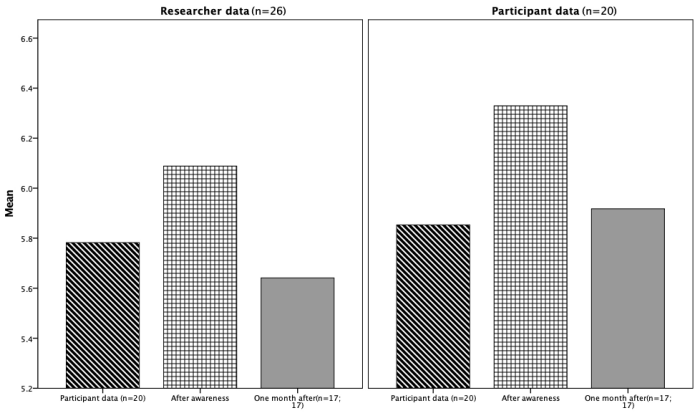

Figure 8: Differences in privacy concerns between participants who used the smart plug themselves to generate their own traffic report, and participants who viewed the researcher's traffic report.

Trust levels in participants (n=20) who agreed to use their own smartphones during the experiment, and those who preferred to use the researcher's home experiment (n=26), were slightly higher, before awareness, in the latter group. However, after being informed of the privacy violations, the situation changed: participants who used their own data had higher levels of trust than the other group. The scenario changed again one month after the experiment, when participants who used the researcher's home experiment results had their trust bounce back to pre-awareness levels (Figure 10). The trust levels before and a month after the experiment demonstrate a small variation (about 0.3), which could indicate that knowledge of the privacy invasion will produce a brief distrusting attitude that will fade over time if the smart device features are still enticing.

4.3. ***RQ.C: Chosen Response Action***

Once the privacy violations were revealed to the participants, they were given the opportunity to respond, adopting one of seven actions, which we will restate here for the sake of clarity: refusal, removal, and misrepresentation (preventative actions); negative word-of-mouth, direct and indirect complaint (disapproval actions); and no response. Our findings show that of the participants (n=46), 39.1% opted to execute private action, 32.6% chose no response, and the rest went for public action.

The results also showed that the participants who chose not to use their own data during the experiment tended not to respond (28.3% of a total 56.5%). On the other hand, 17.4% participants adopted preventative actions, and 10.8% participants adopted disapproval actions. Also, the participants who used their own data during the experiment had a greater tendency to act to prevent the potential privacy violation. 28.2% of participants adopted preventative actions,

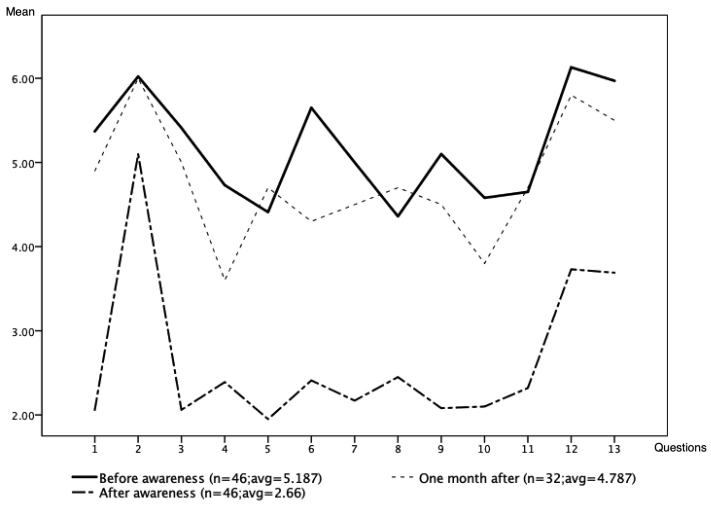

Figure 9: Trust before, after and a month after awareness raising.

10.8% participants adopted disapproval actions, and 4.3% participants chose not to take any action. Figure 11 provides details on the responses selected by participants.

Of the 46 total participants, those who chose to use the researcher's data mainly preferred not to respond to the privacy violation (n=13). Participants that used their own data mainly opted to remove their private data (n=8).

4.3.1. Free Text Responses

Participants were asked to provide reasons for their choices and 16 chose to elaborate on this. In terms of private action, removal (n=7) was selected as the best way to balance the need to protect some personal information with the convenience of a smart device, as illustrated in this sample answer:

> *"Because I still want to use the device in a way that is safe, and to keep my important information protected."*

Negative word-of-mouth was adopted as a response to privacy violations in an altruistic fashion, in an attempt to warn others of the issues:

> *"Because I have a large following on Twitter, so a lot of people will be aware about the privacy issues with smart devices."*

Misrepresentation was selected for similar reasons to removal, i.e. to balance privacy and convenience:

> *"I value my privacy but I love the features of smart devices. This option may give me both."*

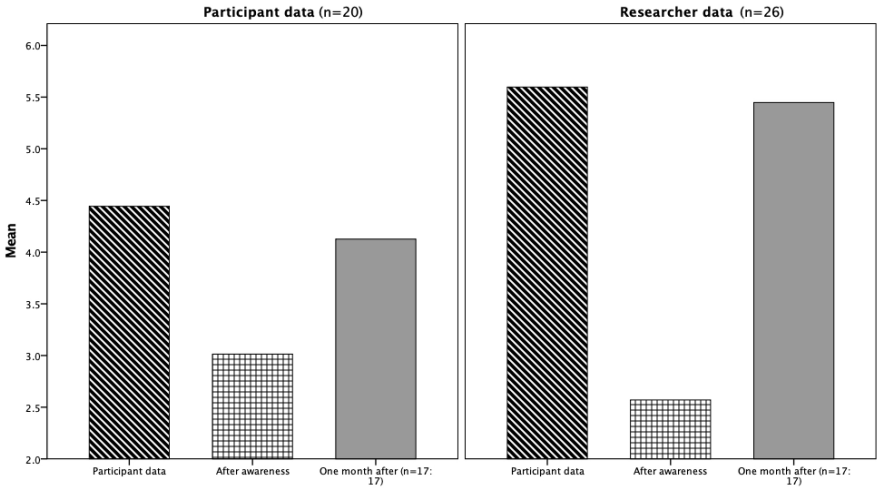

Figure 10: Differences in trust between participants who used their own data, and participants who used the researcher's data.

Refusal was chosen in an unconditional attempt to stop leakage of personal information:

> *"Because I must stop the leaking of information [. . .] to unknown sources."*

In terms of public action, direct complaint was selected in the belief that voicing disappointment would cause the manufacturer to better protect consumers' privacy:

> *"Because I believe they will respond and change their way of treating my personal data".*

The research team also investigated the reasons for some participants not taking action (no response) following awareness of privacy violations (n=15): 7 participants stated that they enjoyed the convenience of smart devices which offset the downsides of privacy violations; 4 stated that they trusted their smart devices despite the violations; and 4 stated that they found the process for protecting their privacy difficult to understand.

4.4. Analysis of Relationships between Constructs

In the present study, we hypothesised that awareness of privacy violations (IV) changes the relationships existing between privacy concerns, trust, and response (DVs). To test these moderating effects, we utilised a repeated measures design (Field, 2013) with one group of participants, by testing the effects of increasing the IoT privacy awareness on privacy concerns, trust and response levels

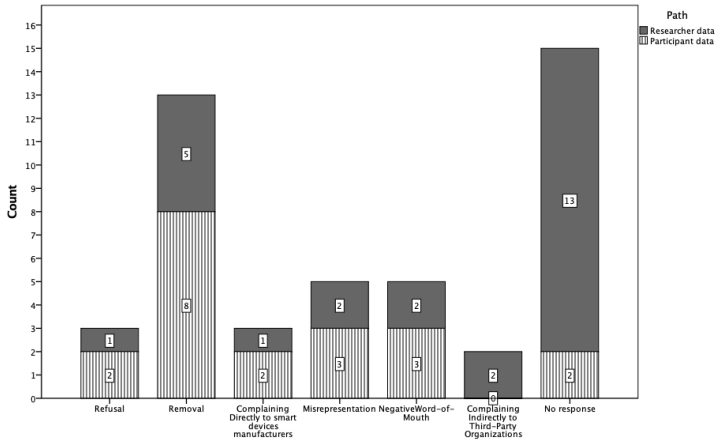

Figure 11: Participants' responses to privacy violations.

of the same group of participants. Standardised values for the DVs were created and, from these, three bivariate correlated relationships were posited applying a non-parametric Spearman's correlation (Field, 2013). The non-parametric test was chosen to match the data's non-normal distribution, based on normality distribution tests being conducted and indicating deviation from normality (e.g. $p < .05$).

Results (see Appendix B) showed that privacy concern was positively associated with trust before intervention on the IV (privacy violations' awareness), with a significant coefficient (r=.352). Manipulation of the IV led to a negative correlation between trust and privacy concerns, with the former decreasing and the latter increasing (r=-.323).

On the other hand, the relationship coefficient among privacy concern, trust and response was too low to be significant (r=-.088; r=-.045). Finally, a month after the end of the experiment, trust was negatively related to privacy concern, with the former increasing and the latter decreasing (r=-.389).

Consequently, multiple Wilcoxon signed-rank, Chi-Square, and one-variable tests (Field, 2013) were conducted to test the hypotheses and provide answers to our research questions. Test results are contained in Appendix C (privacy concerns), Appendix D (trust), and Appendix E (participants' chosen responses).

4.4.1. Kinds of Data

To enrich the data, the researchers asked a participants to provide details on the kinds of personal information that they deemed most sensitive, and hence worth protecting. Participants who selected removal and misrepresentation were required to indicate what personal information they wanted protected at all costs. Credit card details, video recordings, photos and national ID cards were the most often named four categories. Hang et al. (2012) carried out a study to identify the kinds of data people were willing to share. Their participants were

less concerned about sharing timetables, web browsers or camera apps than email, notes, contacts, photos and text messages.

4.5. Considering the Research Questions and Hypotheses

Here, we will report on the research questions and the validated hypotheses.

RQ.A: ***Privacy Concerns.*** *To what extent does a smart device owner's awareness of privacy violations impact their* privacy concerns *when using a device that does not require the upload of private data to enable its functionality?*

If IoT device owners see evidence of IoT privacy violations, their privacy concerns related to smart devices will: not change ($\mathbf{HA}_0$) or increase ($\mathbf{HA}_1$).

The difference between the participants' privacy concerns in the three phases of the experiment (before and after increasing awareness and one month after the experiment concluded) was tested using a Wilcoxon signed-rank test. Privacy concern levels were slightly higher after increasing the privacy awareness than before (Mdn = 6.3 vs. Mdn = 6; r=-0.377, $p < .05$). One month after the experiment, privacy concerns decreased to a lower level than before awareness (Mdn = 5.8; r=-0.248, $p < .05$). Privacy concerns levels also decreased slightly from right after the experiment to a month later = .312) (Asymp. Sig. 2-tailed) (Appendix C).

In conclusion, $\mathbf{HA}_1$ was validated straight after increasing the level of awareness, but $\mathbf{HA}_0$ was validated in the longer term (a month after the experiment).

RQ.B: ***Trust in IoT devices.*** *To what extent does a smart device owner's awareness of privacy violations impact their* trust *in a smart device that does not require to upload private data to enable its functionality?*

If people see evidence of IoT privacy violations, their trust in the smart device will: not change ($\mathbf{HB}_0$) or decrease ($\mathbf{HB}_1$). A Wilcoxon signed-rank test was also utilised to test the trust levels across the experiment. Trust levels were significantly higher before increasing privacy awareness than after (Mdn = 5.6 vs. Mdn = 2.3; r=-0.606, $p < .05$). Trust levels also significantly increased from right after the experiment to one month later (Asymp. Sig. (2-tailed) = .063) (Appendix D).

In conclusion, $\mathbf{HB}_1$ was supported straight after increasing awareness levels, but $\mathbf{HB}_0$ was supported in the longer term (one month after the experiment).

RQ.C: ***Chosen Response Action.*** *To what extent does a smart device owner's awareness of privacy violations impact their* decision to act *to preserve their privacy, and* the nature of the action they take. *This, while using a smart device that does not require the upload of private data to enable its primary functionality?*

If people see evidence of IoT privacy violations, they will: take NO action to prevent them ($\mathbf{HC}_0$), take preventative actions (Refusal, Misrepresentation, Removal) ($\mathbf{HC}_1$) or take disapproval actions (Negative word-of-mouth, Direct complaint, Indirect complaint) ($\mathbf{HC}_2$). A Chi-Squared, one-variable test was

conducted to test the participants' responses to privacy violations. $\mathbf{HC}_0$ was rejected as the value of $p < .05$ (Asymp. Sig. (2-tailed) = 0.024) (Appendix E). In conclusion, there was sufficient evidence to conclude that $\mathbf{HC}_2$ was supported. Table 1 summarises the findings of this study.

Table 1: Hypotheses Summary

DVs	**Measuring Status**	**Mean Ave**	**Hypothesis Supported**	
			After Experiment	**Long-Term**
Privacy Concerns	Before Awareness	5.86	HA_1	HA_0
	After Awareness	6.15		
	A Month Later	5.77		
Trust	Before Awareness	5.18	HB_1	HB_0
	After Awareness	2.66		
	A Month Later	4.78		
Response	Before Awareness	32.6%	HC_2 (disapproval actions)	
	After Awareness	17.4%		
	A Month Later	49.9%		

5. Discussion

Our research showed that participants' concerns and trust in IoT devices changed after their awareness of actual privacy invasions was raised. However, a month after the experiment, privacy concerns and trust regressed to pre-awareness levels.

Data Types: Among the personal information around which participants were most concerned was information that clearly identified them, such as credit card details, video recordings, photos and ID documents. This finding confirms prior research emphasising that consumers seek anonymity to protect their data (55% of Internet users opt for this solution) (Rainie et al., 2013). Trust in the IoT smart device was significantly higher before awareness raising (avg=5.18), an element further confirmed by the fact that none of the 46 participants read the privacy policy provided with the smart device during the preamble phase.

Explaining the Findings: An explanation of this level of trust is offered by the literature suggesting the determinant role of perceived benefits in assessing the risks associated with privacy violations (Hsu and Lin, 2016; Barth et al., 2019). In essence, convenience and benefits accruing from use of IoT devices have, so far, outweighed their owners' concerns. This is reminiscent of the role of perceived usefulness in the Technology Acceptance Model (Davis, 1989). At a deeper level of analysis, however, our findings seem to confirm the activation of the privacy paradox stemming from behavioural economics disciplines.

Phelan et al. (2016) explain the privacy paradox by splitting privacy concerns into two components: intuitive concerns (stemming from Kahneman's System 1 way of thinking (Kahneman, 2003): fast, automatic processes) and considered

concerns (stemming from Kahneman's System 2 way of thinking (Kahneman, 2003): which are driven by a reasoned, deliberate process where judgements derive from logic and rationality. According to this perspective, considered concerns are time consuming so the privacy paradox derives from a failure to engage in a time consuming consideration of one's actions. Choi et al. (2018) argue that people are suffering from *privacy fatigue*, leading to disengagement and a failure to carry out privacy protecting behaviours.

Privacy Policies: In our research, participants' failure to read the privacy policy provided with the IoT smart device appears to confirm that the participants were guided by System 1 thinking, associated with intuitive concerns (the privacy policy being too long and complicated to be worth reading). This also confirms what Herley (2009) argues: that people engage in perfectly rational trade-offs based on the excessive effort required to take action.

The research literature argues that the digital world, with its fast-paced rhythm, has pushed individuals towards System 1 thinking even more (Kahneman, 2003) and the widespread diffusion of the IoT seems to exacerbate this trend. As illustrated in Figure 4, we formulated the privacy policy in a typically wordy, vague and non-plain language, to epitomise the nature of most privacy policies attached to IoT smart devices[1]. We did not ask participants why they did not read the privacy policy; our observation of non-reading confirms those of other researchers (Vila et al., 2003; Obar and Oeldorf-Hirsch, 2018). Explanations for this neglect include expectations of poor understandability (Pierce et al., 2018; Paul et al., 2018), and a sense of helplessness (Fast and Jago, 2019), reading these being a nuisance and an obstacle in the way of goal satisfaction (Obar and Oeldorf-Hirsch, 2018).

They might also have been eager to conclude the experiment in the least amount of time, or may have trusted the experimenter and thought that reading the policy would implicitly insult her. Regardless of the reasons, our investigation does emphasise the importance of user-friendliness in the design and drafting of IoT smart devices' privacy policies, a recommendation also made in recent research (Cha et al., 2018) and promoted through legislation (Vijayan, 2005). A clear and credible privacy policy (as noted by Vijayan (2005)) could help vendors to build more positive relationships with consumers.

Bounded Rationality: Our study also confirms findings from the behavioural economics literature, in particular around the concept of bounded rationality. Decisions are affected by heuristic and cognitive preferences such as optimism and affection bias, overconfidence, benefit heuristics or exaggerated discounting (Strough et al., 2011). Our participants demonstrated a degree of uncertainty in how they assessed privacy violations by the IoT smart device, either because of incomplete information (how would they know what use third-party companies would make of their personal information?) or cognitive limitations (how would positive emotions associated with the usage of a smart

[1] `https://www.gdprtoday.org/privacy-policies-for-internet-of-things-devices-must-comply-with-gdpr/`

device influence the assessment of risks associated with privacy violations?) (Kehr et al., 2015).

Durability of Concern and Trust Adjustments: At the commencement of the experiment, we used Cheung and Lee's instrument (2000) to measure participants' level of trust and to assess how our IV (privacy awareness) impacted this. Our research showed that privacy concerns increased and trust levels decreased after privacy violations were disclosed. This answers a question yet to be addressed in the literature: "*how long would it take for an end-user to lower their concern threshold and re-establish their trust in a smart device after becoming aware of a privacy violation?*" Our study sets the threshold at, or less than, a month, after which privacy concerns and trust rebounded to pre-violation awareness levels.

In Summary: Two practical implications emerge from this. *First*, from an organisational perspective, companies willing to monitor employees' attitudes towards smart devices and to identify instances of negligence (e.g., improper usage leading to leakage of personal information) may want to organise 'refresher training' once a month, to ensure a 'healthy level of concern' is maintained. *Second*, from a business perspective, organisations willing to recover from adverse publicity deriving from unwanted disclosure of consumers' personal information need to focus their restoration efforts within the month after the adverse event.

5.1. Chosen Responses to Increased Privacy Violation Awareness

While previous studies have indicated that privacy issues have a significant impact on consumers' willingness to utilise IoT devices, our research confirms more recent findings on the unreliability of responses flowing from this impact (Hsu and Lin, 2016).

From a theoretical perspective, our investigation has expanded our understanding of how people respond to evidence of privacy violations. The fact that only 3 participants, out of 46, unconditionally discontinued usage of the IoT smart device (refusal) and 28 decided to protect their privacy, yet without sacrificing the smart features offered by the device using disapproval actions. This indicates that the perceived benefits of the smart device were still too high for owners to sacrifice its functionality. This is consistent with the literature on the so-called *privacy calculus* which suggests that when comparing risks and benefits, individuals often underestimate the former and overestimate the latter (Kim et al., 2019; Pavlou, 2011; Kehr et al., 2015). Lack of a legislative framework to promote privacy protection could be another factor to consider in the bigger picture. Saudi Arabia currently has no specific data protection legislation, except for laws grounded in the principles of governance and sector-specific legislative instruments (Royal Order No. (A/91), 1992). These laws are not designed to protect consumers in the case of IoT privacy infringement cases (Alsulaiman and Alrodhan, 2014). Participants in our study largely decided not to act when informed of the privacy violations perpetrated by the IoT smart device. Yet, we could hypothesise that the existence of a legislative framework obliging public and private organisations to take proactive actions to better

protect people's privacy (with significant penalties to punish abuse) might well increase willingness to respond.

5.2. Limitations and Future Research

The main limitation of this study resides in its sample, confined to a specific geographical area, and relatively small in size. This could translate to reduced generalisability of the findings. Level of analysis was another limiting factor. Since this study was based on privacy concerns and trust as antecedents to participants' responses to privacy violations, there could potentially be more factors coming into play, such as, for example, individual background, age, gender, social and milieu influences, personality traits, etc. We suggest further research to examine the impact of these additional variables to expand our understanding of attitudes *vis-á-vis* IoT smart devices and privacy violations. Responding to calls in the literature for a less logically centred approach to such investigations (Hsu and Lin, 2016), our study has focused on individual and socially constructed factors. We believe this is a promising avenue for future research.

5.3. Ethics

Ethical approval for this study was obtained from the University of [Anonymised]. In particular, this required the research team to offer alternative paths (A) and (B) during the experiment, so that people could still participate even if they did not want to install the IoT device app on their own smartphones. This respected their need to preserve their own privacy but still to be informed of potential privacy violations. All responses provided in this investigation were treated anonymously and participants' network traffic analysis was deleted at the end of the experiment.

6. Conclusion

The privacy paradox is a well known phenomenon, reflecting the puzzling mismatch between stated privacy concerns and the absence of actual privacy protecting behaviours.

We wanted to determine whether this would also manifest in the IoT domain. We thus carried out a study to determine what actions people would choose to carry out in the face of evidence of actual privacy violations committed by an IoT device. Our participants were shown evidence of potential privacy leakage by a smart plug, then we asked them to choose an action, which ranged from discontinuing usage to mere disapproval. We also measured privacy concerns and trust both before and after they saw this evidence.

Our participants generally did not want to discontinue using the device, most preferring to express their disapproval while retaining the device. While their privacy concerns increased and trust decreased immediately after the experiment, both regressed to pre-awareness levels a month later.

Our findings confirm that the privacy paradox also manifests in the IoT domain. This is particularly concerning because these devices are in our homes, our most personal and private spaces, and have the potential to commit the worst kinds of privacy invasions. It is clear that a mere increase in awareness is not going to convince everyone to take action to preserve their privacy. Awareness, on its own, is often insufficient to prompt action. As a next step, we ought to experiment with different ways of motivating people to take action to prevent these kinds of privacy invasions, and no longer naïvely put our faith in increasing awareness.

Acknowledgements

We are grateful for the funding provided by the Saudi Arabian Cultural Mission, which made it possible for this research to be carried out.

References

Noura Aleisa and Karen Renaud. Privacy of the Internet of Things: A Systematic Literature Review. In *50th Annual Hawaii International Conference on System Sciences (HICSS)*, The Big Island, Hawai'i, 2017a. IEEE.

Noura Aleisa and Karen Renaud. Yes, I know this IoT Device Might Invade my Privacy, but I Love it Anyway! A Study of Saudi Arabian Perceptions. In *2nd Intl Conference on Internet of Things. 24-26 April*, pages 198–205., Porto, Portugal, 2017b.

Areej AlHogail. Improving IoT technology adoption through improving consumer trust. *Technologies*, 6(3):64, 2018.

Laith A Alsulaiman and Waleed A Alrodhan. Information Privacy Status in Saudi Arabia. *Computer and Information Science*, 7(3):102–124, 2014.

Hany F Atlam and Gary B Wills. IoT Security, privacy, safety and ethics. In *Digital Twin Technologies and Smart Cities*, pages 123–149. Springer, 2020.

Susan B Barnes. A privacy paradox: Social networking in the United States. *First Monday*, 11(9), 2006.

Susanne Barth, Menno D.T. de Jong, Marianne Junger, Pieter H Hartel, and Janina C Roppelt. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, 41:55–69, 2019.

Emma Bell, Alan Bryman, and Bill Harley. *Business research methods*. Oxford University Press, 2018.

Rachel Botsman. *Who can you trust? How technology brought us together–and why it could drive us apart*. Penguin UK, 2017.

Lucie C Burgess, Anya Skatova, Sinong Ma, Rebecca McDonald, and Carsten Maple. The Value of Personal Data in IoT: Industry Perspectives on Consumer Conceptions of Value. In *Living in the Internet of Things (IoT 2019)*, London, UK, 1-2 May 2019. IET.

Shi-Cho Cha, Ming-Shiung Chuang, Kuo-Hui Yeh, Zi-Jia Huang, and Chunhua Su. A user-friendly privacy framework for users to achieve consents with nearby BLE devices. *IEEE Access*, 6:20779–20787, 2018.

Ravishankar Chamarajnagar and Ashwin Ashok. Privacy Invasion through Smarthome IoT Sensing. In *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pages 1–9. IEEE, 2019.

Sunil Cheruvu, Anil Kumar, Ned Smith, and David M Wheeler. *Demystifying Internet of Things Security: Successful IoT Device/Edge and Platform Security Deployment*. Apress, 2019.

Christy Cheung and Matthew K.O. Lee. Trust in Internet shopping: A proposed model and measurement instrument. In *Proceedings AMCIS*, page 406, Westin Hotel, Long Beach, 2000.

Hanbyul Choi, Jonghwa Park, and Yoonhyuk Jung. The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81:42–51, 2018.

Rory Coulter and Lei Pan. Intelligent agents defending for an IoT world: A review. *Computers & Security*, 73:439–458, 2018.

Richard P.; Warshaw Paul R. Davis, Fred D.; Bagozzi. User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, 35(8):982–1003, 1989.

Shravani Devarakonda, Malka N Halgamuge, and Azeem Mohammad. Critical issues in the invasion of the Internet of Things (IoT): Security, privacy, and other vulnerabilities. In *Handbook of Research on Big Data and the IoT*, pages 174–196. IGI Global, 2019.

Tobias Dienlin and Sabine Trepte. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, 45(3):285–297, 2015.

Sandra Dominikus. MedAssist - A privacy preserving application using RFID tags. In *International Conference on RFID-Technologies and Applications (RFID-TA)*, pages 370–375. IEEE, 2011.

Ike C Ehie and Michael A Chilton. Understanding the influence of IT/OT Convergence on the adoption of Internet of Things (IoT) in manufacturing organizations: An empirical investigation. *Computers in Industry*, 115:103166, 2020.

Waleed Ejaz and Alagan Anpalagan. *Internet of things for smart cities: technologies, big data and security*. Springer, Kamloops, BC, Canada, 2019.

EU Parliament. Home Page of EU GDPR, 2018. `https://www.eugdpr.org/`(Accessed April 2018).

Nathanael J Fast and Arthur S Jago. Privacy matters... Or does it? Algorithms, rationalization, and the erosion of concern for privacy. *Current Opinion in Psychology*, 2019.

Andy Field. *Discovering statistics using IBM SPSS statistics*. Sage, 2013.

Lingling Gao and Xuesong Bai. A unified perspective on the factors influencing consumer acceptance of Internet of Things technology. *Asia Pacific Journal of Marketing and Logistics*, 26(2):211–231, 2014.

Nina Gerber, Paul Gerber, and Melanie Volkamer. Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77:226–261, 2018.

Mehdi Gheisariy, Guojun Wang, Wazir Zada Khanz, and Christian Fernández-Campusano. A context-aware privacy-preserving method for IoT-based smart city using Software Defined Networking. *Computers & Security*, 2019.

Bo Han, Yu Andy Wu, and John Windsor. User's adoption of free third-party security apps. *Journal of Computer Information Systems*, 54(3):77–86, 2014.

Alina Hang, Emanuel Von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. Too much information! User attitudes towards smartphone sharing. In *Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design*, pages 284–287. ACM, 2012.

Martin Henze, Lars Hermerschmidt, Daniel Kerpen, Roger Häußling, Bernhard Rumpe, and Klaus Wehrle. A comprehensive approach to privacy in the cloud-based Internet of Things. *Future Generation Computer Systems*, 56: 701–718, 2016.

Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *New Security Paradigms Workshop*, pages 133–144. ACM, 2009.

Chin-Lung Hsu and Judy Chuan-Chuan Lin. An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behavior*, 62: 516–527, 2016.

Internet Society. The trust opportunity: Exploring consumers' attitudes to the internet of things, 2019. `https://www.internetsociety.org/wp-content/uploads/2019/05/CI_IS_Joint_Report-EN.pdf` Accessed 3 March 2020.

Daniel Kahneman. A perspective on judgment and choice: Mapping bounded rationality. *American Psychologist*, 58(9):697–720, 2003.

Jiawen Kang, Rong Yu, Xumin Huang, and Yan Zhang. Privacy-preserved pseudonym scheme for fog computing supported Internet of Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 19(8):2627–2637, 2017.

Yu-Sheng Kao, Kazumitsu Nawata, and Chi-Yo Huang. An exploration and confirmation of the factors influencing adoption of IoT-based wearable Fitness trackers. *International Journal of Environmental Research and Public Health*, 16(18):3227, 2019.

Flavius Kehr, Tobias Kowatsch, Daniel Wentzel, and Elgar Fleisch. Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, 25(6):20779–20787, 2015.

Bilal Khan, Khaled S Alghathbar, Syed Irfan Nabi, and Muhammad Khurram Khan. Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, 5(26): 10862–10868, 2011.

Dongyeon Kim, Kyuhong Park, Yongjin Park, and Jae-Hyeon Ahn. Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, 92:273–281, 2019.

Agnieszka Kitkowska, Erik Wästlund, Joachim Meyer, and Leonardo A Martucci. Is it harmful? Re-examining privacy concerns. In *IFIP International Summer School on Privacy and Identity Management*, pages 59–75. Springer, 2017.

Geir M Køien. Reflections on trust in devices: an informal survey of human trust in an Internet-of-Things context. *Wireless Personal Communications*, 61(3):495–510, 2011.

Martin J Kraemer and Ivan Flechais. Researching privacy in smart homes: A roadmap of future directions and research methods. In *IET Living in the Internet of Things: Cybersecurity of the IoT Conference*, 2018.

Naresh K Malhotra, Sung S Kim, and James Agarwal. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, 15(4):336–355, 2004.

Argyro Mavrogiorgou, Athanasios Kiourtis, Konstantinos Perakis, Stamatios Pitsios, and Dimosthenis Kyriazis. IoT in Healthcare: Achieving Interoperability of High-Quality Data Acquired by IoT Medical Devices. *Sensors*, 19 (9):1978, 2019.

Roger C Mayer, James H Davis, and F David Schoorman. An integrative model of organizational trust. *Academy of Management Review*, 20(3):709–734, 1995.

Francesca Meneghello, Matteo Calore, Daniel Zucchetto, Michele Polese, and Andrea Zanella. IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal*, 6(5): 8182–8201, 2019.

Shaun Mirani, Joshua Meyer, Rick Ramgattie, and Ian Sindermann. Security vulnerabilities in network accessible services, 2019. `https://www.ise.io/casestudies/sohopelessly-broken-2-0/` Accessed 3 March 2020.

Hooman Mohajeri Moghaddam, Gunes Acar, Ben Burgess, Arunesh Mathur, Danny Yuxing Huang, Nick Feamster, Edward W Felten, Prateek Mittal, and Arvind Narayanan. Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 131–147, 2019.

Norshidah Mohamed and Ili Hawa Ahmad. Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, 28(6):2366–2375, 2012.

Patricia A Norberg, Daniel R Horne, and David A Horne. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1):100–126, 2007.

Jonathan A Obar and Anne Oeldorf-Hirsch. The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, pages 1–20, 2018.

Robert Oshana and Mark Kraeling. *Software engineering for embedded systems: Methods, practical techniques, and applications*. Newnes, Oxford, UK, 2019.

Niklas Paul, Welderufael B Tesfay, Dennis-Kenji Kipker, Mattea Stelter, and Sebastian Pape. Assessing Privacy Policies of Internet of Things Services. In *IFIP International Conference on ICT Systems Security and Privacy Protection*, pages 156–169. Springer, 2018.

Paul A Pavlou. State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, 35(4):977–988, 2011.

Chanda Phelan, Cliff Lampe, and Paul Resnick. It's creepy, but it doesn't bother me. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 5240–5251. ACM, 2016.

James Pierce, Sarah Fox, Nick Merrill, Richmond Wong, and Carl DiSalvo. An interface without a user: An exploratory design study of online privacy policies and digital legalese. In *Proceedings of the 2018 Designing Interactive Systems Conference*, DIS '18, pages 1345–1358, New York, NY, USA, 2018. ACM. URL `http://doi.acm.org/10.1145/3196709.3196818`.

Lee Rainie, Sara Kiesler, Ruogu Kang, Mary Madden, Maeve Duggan, Stephanie Brown, and Laura Dabbish. Anonymity, privacy, and security online, 2013. Pew Research Center `http://pewinternet.org/Reports/2013/Anonymity-online.aspx` Accessed 17 April 2020.

Jingjing Ren, Daniel J Dubois, David Choffnes, Anna Maria Mandalari, Roman Kolcun, and Hamed Haddadi. Information exposure from consumer IOT devices: A multidimensional, network-informed measurement approach. In *Proceedings of the Internet Measurement Conference*, pages 267–279, 2019.

Royal Order No. (A/91). Basic Law of Governance, 1992. `https://www.wipo.int/edocs/lexdocs/laws/en/sa/sa016en.pdf` Accessed 20 November 2019.

Neil J Salkind. *Encyclopedia of Research Design*, volume 2. Sage, 2010.

Florian Schaub, Rebecca Balebako, Adam L Durity, and Lorrie Faith Cranor. A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS)*, pages 1–17, 2015.

H Jeff Smith, Tamara Dinev, and Heng Xu. Information privacy research: an interdisciplinary review. *MIS Quarterly*, 35(4):989–1016, 2011.

Jai-Yeol Son and Sung S Kim. Internet users' information privacy-protective responses: A taxonomy and a nomological model. *MIS Quarterly*, 32(3): 503–529, 2008.

Statista. Number of smartphone users in Saudi Arabia from 2017 to 2023 (in millions), 2019. `https://www.statista.com/statistics/494616/smartphone-users-in-saudi-arabia/` Accessed February 2020.

JoNell Strough, Tara E Karns, and Leo Schlosnagle. Decision-making heuristics and biases across the life span. *Annals of the New York Academy of Sciences*, 1235:57, 2011.

Telecom Review. Research shows rapid adoption of IoT in UAE and KSA, 2018. http://www.telecomreview.com/index.php/articles/reports-and-coverage/2522-research-shows-rapid-adoption-of-iot-in-uae-and-ksa Accessed 17 April 2020.

Krystan ten Berg, Ton AM Spil, and Robin Effing. The Privacy Paradox of Utilizing the Internet of Things and Wi-Fi Tracking in Smart Cities. In *International Working Conference on Transfer and Diffusion of IT*, pages 364–381. Springer, 2019.

Jeevan Thankappan. Saudi smartphone penetration exceeds global average, 2017. `https://www.tahawultech.com/news/saudi-smartphone-penetration-exceeds-global-average/` Accessed 15 November 2019.

Sabine Trepte, Tobias Dienlin, and Leonard Reinecke. Risky behaviors: How online experiences influence privacy behaviors. *Von Der Gutenberg-Galaxis Zur Google-Galaxis. From the Gutenberg Galaxy to the Google Galaxy*, 2014.

Jaikumar Vijayan. Companies simplify data privacy notices: P & G, Microsoft are in forefront of move to make web site disclosures more user-friendly. *Computerworld 10 January 2005*, 39(2):1, 2005.

Tony Vila, Rachel Greenstadt, and David Molnar. Why we can't be bothered to read privacy policies models of privacy economics as a lemons market. In *Proceedings of the 5th International Conference on Electronic Commerce*, pages 403–407. ACM, 2003.

Alan F. Westin. *Privacy and Freedom*. Atheneum, New York, 1967.

Dino Wilkinson and Saud Alsaab. Data protection in Saudi Arabia: overview, 2019. OneTrust Data Guidance `https://platform.dataguidance.com/notes/saudi-arabia-data-protection-overview` Accessed 17 April 2020.

Meredydd Williams. *Exploring the influence of privacy awareness on the Privacy Paradox on smartwatches*. PhD thesis, University of Oxford, 2018.

Meredydd Williams, Jason RC Nurse, and Sadie Creese. The perfect storm: The privacy paradox and the Internet-of-Things. In *11th International Conference on Availability, Reliability and Security (ARES)*, pages 644–652. IEEE, 2016.

Zheng Yan, Peng Zhang, and Athanasios V Vasilakos. A survey on trust management for Internet of Things. *Journal of Network and Computer Applications*, 42:120–134, 2014.

Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. User perceptions of smart home IoT privacy. In *Proceedings of the ACM on Human-Computer Interaction*, volume 2. ACM, 2018. `https://doi.org/10.1145/3274469`.

Appendix A. Construct Measurement Questions

Appendix A.1. Trust in IoT Measurement

Here are some statements about personal information. From the standpoint of personal privacy, please indicate the extent to which you, as an individual, agree or disagree with each statement by circling the appropriate number. Each of the items is followed by a seven-point Likert scale anchored by "strongly disagree" and "strongly agree".

Table A.2: Trust Questions

1. Internet of Things vendors implement security measures to protect their users.
2. Internet of Things vendors have the ability to verify Internet of Things users' identity for security purpose.
3. Internet of Things vendors usually ensure that transactional information is protected from accidentally altered or destroyed during transmission on the Internet.
4. Internet of Things vendors will not sell my personal information to the third parties without my permission.
5. Internet of Things vendors concern about consumers privacy.
6. Internet of Things vendors will not divulge consumers personal data to other parties.
7. I feel safe about the privacy control of Internet of Things vendors.
8. It is easy for me to trust a person/thing.
9. My tendency to trust a person/thing is high.
10. I tend to trust a person/thing, even though I have little knowledge of it.
11. Trusting someone or something is not difficult.
12. Using the smart devices has been a good experience to me personally.
13. I have positive experiences of using the smart devices.

Appendix A.2. Response Actions

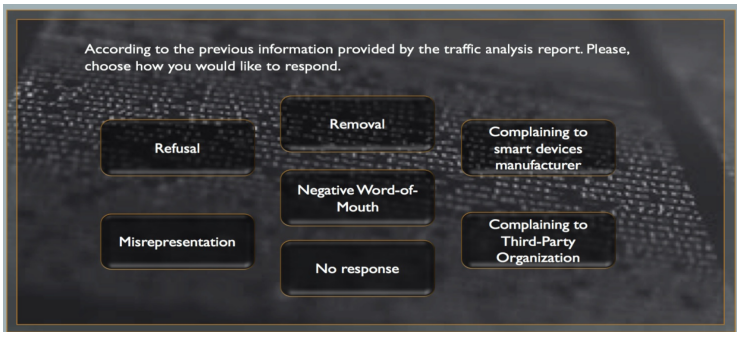

Figure A.12: Offering Participants a Choice of Response Actions

Due to space limitations we direct the reader to [Anonymised for Review] for details of exactly what the interface looked like for each of these chosen options.

Appendix A.3. Privacy Concerns to IoT Measurement

Here are some statements about personal information. From the standpoint of personal privacy, please indicate the extent to which you, as an individual, agree or disagree with each statement by circling the appropriate number.* Each of the items is followed by a seven-point Likert scale anchored by "strongly disagree" and "strongly agree".

Table A.3: Privacy Concern Questions

Control
1. Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
2. Consumer control of personal information lies at the heart of consumer privacy.
3. I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction. Awareness (of privacy practices):
Awareness
1. Companies seeking information online should disclose the way the data are collected, processed, and used.
2. A good consumer online privacy policy should have a clear and conspicuous disclosure.
3. It is very important to me that I am aware and knowledgeable about how my personal information will be used.
Collection
1. It usually bothers me when companies ask me for personal information.
2. When online companies ask me for personal information, I sometimes think twice before providing it.
3. It bothers me to give personal information to so many online companies.
4. I'm concerned that online companies are collecting too much personal information about me.

Appendix B. Tests of moderating effects among variables

			Trust B Mean	Perception B Mean
Spearman's Rho	Trust B Mean	Correlation Coefficient	.352*	1.000
		Sig. (2-tailed)	.016	.
		N	46	46
	Trust B Mean	Correlation Coefficient	1.000	.352*
		Sig. (2-tailed)	.	.016
		N	46	46

Table B.4: Relationship between trust and privacy concerns before awareness raising.

			Trust A Mean	Perception A Mean	Response
Spearman's Rho	Trust A Mean	Correlation Coefficient	1.000	-.323*	-.088
		Sig (2-tailed)	.	.029	.561
		N	46	46	46
	Perception A Mean	Correlation Coefficient	-.323*	1.000	-.045
		Sig (2-tailed)	.029	.	.766
		N	46	46	46
	Response	Correlation Coefficient	-.088	-.045	1.000
		Sig (2-tailed)	.561	.766	1.000
		N	46	46	46

Table B.5: Relationship between trust, privacy concerns and responses after awareness.

			Trust M Mean	Perception B Mean
Spearman's Rho	Trust M Mean	Correlation Coefficient	1.000	-.389*
		Sig. (2-tailed)	.	.023
		N	14	34
	Trust B Mean	Correlation Coefficient	-.389	1.000
		Sig. (2-tailed)	.023	.
		N	34	34

Table B.6: Relationship between trust and privacy concerns a month after awareness raising.

Appendix C. Privacy concerns – Wilcoxon signed-rank test outputs

		N	Mean Rank	Sum of Ranks
Privacy Concern after Awareness - Privacy Concern before Awareness	Negative Ranks	9[a]	20.61	185.50
	Positive Ranks	35[b]	22.99	804.50
	Ties	2[c]		
	Total	46		
Privacy Concern Month after Awareness - Privacy Concern before Awareness	Negative Ranks	19[d]	16.74	318.00
	Positive Ranks	13[e]	16.15	210.00
	Ties	2[f]		
	Total	34		
Privacy Concern Month after Awareness - Privacy Concern After Awareness	Negative Ranks	22[g]	16.41	361.00
	Positive Ranks	9[h]	15.00	135.00
	Ties	3[i]		
	Total	34		

a. PCAA < PCBA; b. PCAA > PCBA; c. PCAA = PCBA; d. PCMAA < PCBA; e. PCMAA > PCBA; f. PCMAA = PCBA; g. PCMAA < PCAA; h. PCMAA > PCAA; i. PCMAA = PCAA;

Table C.7: Ranks (PCAW=Privacy Concern After Awareness; PCBA=Privacy Concern Before Awareness; PCMAA=Privacy Concern Month After Awareness)

	Privacy Concern After Awareness - Privacy Concern Before Awareness	Privacy Concern Month After Awareness - Privacy Concern Before Awareness	Privacy Concern Month After Awareness - Privacy Concern After Awareness
Z	-3.621[a]	-1.010[b]	-2.218[c]
Asymp Sig (2-tailed)	.000	.312	.027
Exact Sig (2-tailed)	.000	.319	.025
Exact Sig (1-tailed)	.000	.160	.013
Point Probability	.000	.002	.000

a Wilcoxon Signed Ranks Test; *b* Based on negative ranks; *c* Based on positive ranks

Table C.8: Test statistics.

Appendix D. Trust – Wilcoxon signed-rank test outputs

		N	Mean Rank	Sum of Ranks
Trust after Awareness - Trust before Awareness	Negative Ranks	44[a]	23.45	1032.50
	Positive Ranks	1[b]	3.00	3.00
	Ties	1[c]		
	Total	46		
Trust Month after Awareness - Trust After Awareness	Negative Ranks	23[d]	15.80	363.50
	Positive Ranks	9[e]	15.00	135.00
	Ties	2[f]		
	Total	34		
Trust Month after Awareness - Trust before Awareness	Negative Ranks	1[g]	2.00	2.00
	Positive Ranks	33[h]	17.97	593.00
	Ties	0[i]		
	Total	34		

a. TAA < TBA; b. TAA > TBA; c. TAA = TBA; d. TMAW < TBA; e. TMAW > TBA; f. TMAW = TBA; g. TMAW < TAA; h. TMAW > TAA; i. TMAW = TAA

Table D.9: Trust ranks (TAA=Trust After Awareness; TBA=Trust Before Awareness; TMAA=Trust Month After Awareness).

	Trust After Awareness - Trust Before Awareness	Trust Month After Awareness - Trust Before Awareness	Trust Month After Awareness - Trust After Awareness
Z	-5.809[a]	-1.861[b]	-5.053[c]
Asymp Sig (2-tailed)	.000	.063	.000
Exact Sig (2-tailed)	.000	.063	.000
Exact Sig (1-tailed)	.000	.031	.000
Point Probability	.000	.001	.000

a Wilcoxon Signed Ranks Test; *b* Based on negative ranks; *c* Based on positive ranks

Table D.10: Trust test statistics.

Appendix E. Participants' responses and responses categories – Chi-Squared, one-variable test outputs

	Observed N	Expected N	Residual
Refusal	3	6.6	-3.6
Removal	13	6.6	6.4
Misrepresentation	5	6.6	-1.6
Complaining to Smart Device Manufacturer	3	6.6	-3.6
Negative Word of Mouth	5	6.6	-1.6
Complaining to 3rd Party Orgs	2	6.6	-4.6
No Response	15	6.6	8.4
Total	46		

Table E.11: Participant behavioural responses.

	Responses
Chi-Square	24.913[a]
df	6

Asymp. Sig.	.000
Exact Sig	.000
Point Probability	.000

a 0 cells (0.0%) have expected frequencies; less than 5. The minimum expected cell frequency is 6.6.

Table E.12: Test statistics.

	Response Category	Expected N	Residual
Public Action	5	11.5	-6.5
Private Action	18	11.5	6.5
Information Provision	8	11.5	-3.5
No Action	15	11.5	3.5
Total	46		

Table E.13: Participant behavioural response categories.

	Response Category
Chi-Square	9.478[a]
df	3

Asymp. Sig.	.024
Exact Sig	.022
Point Probability	.002

[a] 0 cells (0.0%) have expected frequencies; less than 5. The minimum expected cell frequency is 11.6.

Table E.14: Test statistics.